研究論文

鳴門教育大学情報教育ジャーナル 5, 1-6, 2008

Proxy サーバによる HTTP トラフィックのルーティング

曽根直人*，林　秀彦*，菊地　章*,**

本学では，拡大するインターネット向けトラフィックへの対応，および工事などによるインターネット接続の停止期間を減少させるため，従来の SINET 回線に加えて新たに商用インターネット回線とも接続を行い，学内 LAN とインターネットの接続を冗長化した。複数のネットワーク経路を有効に活用するため，HTTP Proxy サーバを利用したアプリケーション層での経路制御を行い，HTTP トラフィックの一部を商用ネットワークへルーティングすることでトラフィックの分散を図り，複数経路の有効利用を試みている。

[**キーワード**: HTTP Proxy，マルチホーム，ポリシールーティング]

1．はじめに

今日ではインターネットは重要な社会基盤の一つとして研究・教育活動のみならず，さまざまな情報の提供や交換に日々利用されている。本学においてもインターネット接続に関連する機材はメンテナンス時を除き常時稼働しており，学内のユーザに対するインターネット接続を提供している。しかし，本学のインターネット接続は単独の上位ネットワークと接続するシングルホーム接続であり，上位ネットワークである SINET とは徳島ノード経由でのみ接続されている。そのため工事などで SINET が停止する期間，本学はインターネットへの接続を失うことになる。特にノード校の停電時には日中数時間にわたって本学からインターネットへの接続が失われるため，利用者から改善を望む声が多く寄せられていた。

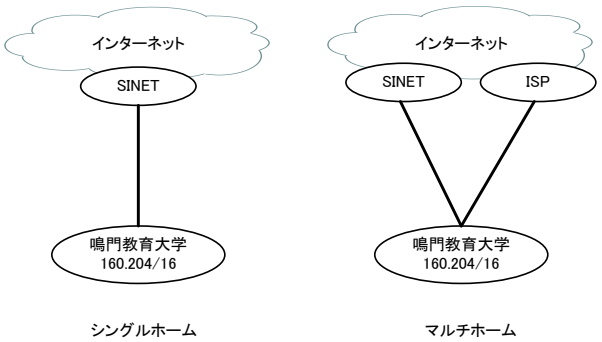

図 1　シングルホーム，マルチホーム

高度情報研究教育センターでは，より安定したインターネット接続を実現するために，SINET に加えて商用インターネットサービスプロバイダ(ISP)を上位ネットワークとして接続し，インターネット接続を冗長化するマルチホーム接続を望んでいた。しかし高島地区では地理的な問題から安価なブロードバンドサービスが提供されておらず，実現には至らなかった。2007 年になり，ようやく高島地区でも安価なブロードバンドサービスの提供が始まったことを受け，本センターでも 2007 年 10 月より商用 ISP と契約を行いインターネット接続回線の冗長化を実現した。

我々は冗長化したインターネット接続を有効に利用するため，最も多く利用されているアプリケーションである Web のトラフィックに注目した。本稿では Proxy サーバを用いて学外 Web サーバへのアクセスを冗長化されたインターネット回線に振り分け，負荷を分散させるためのトラフィックルーティング方法について述べる。

2．ネットワーク構成

本学のネットワーク論理構成を図 2 に示す。

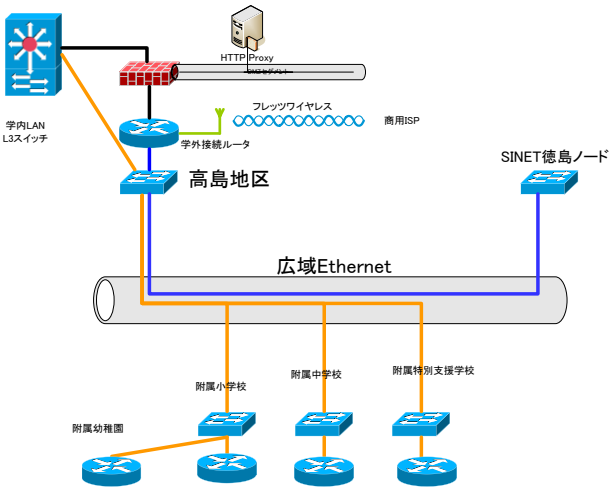

図 2　ネットワーク論理構成

インターネット接続はマルチホーム構成になっており，上位ネットワークとして SINET，商用 ISP の 2 系統が存在する。学外接続ルータには 2 系統の上位ネットワークがそ

*　鳴門教育大学　高度情報研究教育センター
**　鳴門教育大学　生活・健康系（技術）教育講座

れぞれ接続されている。ファイヤーウォールは学外接続ルータと学内LANを接続する位置にあり，DMZセグメントにはHTTP Proxyサーバ他いくつかのサーバが接続されている。

SINET 徳島ノード(徳島大学内)との接続に用いているのは広域Ethernetサービス(100Mbps)回線である。ただし，この回線はタグVLANを用いて論理的に多重化しており，100Mbpsの帯域を高島地区とSINET徳島ノード間を結ぶネットワークおよび高島地区と附属学校・園間を結ぶネットワークが共有している。

商用回線は高島地区で利用可能なブロードバンド接続サービスの一つであるNTT西日本Bフレッツワイヤレスタイプ［1]を用いてISP(BIGLOBE社)と接続している。この回線はFWA(固定無線)回線を利用しており，無線最大伝送速度最大80Mbps，実行速度下り最大46Mbpsの帯域を提供する。加入者用アンテナは本センターの屋上に設置している。設置場所と基地局アンテナは150m程度の距離であり，障害物もなく目視で確認できる状態(図 3)である。

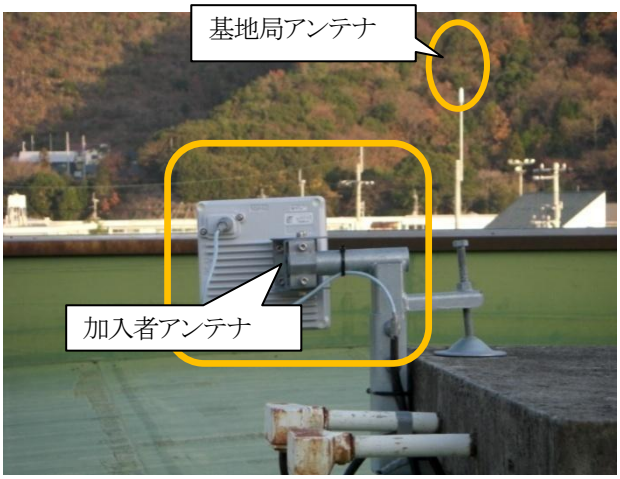

図 3　FWA用アンテナ

3．HTTPトラフィックルーティング

3．1　マルチホーム接続

SINET に加えて商用回線と契約したことにより，本学はインターネットへの接続経路を複数持つことになった。しかし，単純にインターネットへの接続を商用ISPにも割り振った場合，懸案であったSINET停止時の対策とはならない。なぜなら，本学のネットワークアドレス(160.204.0.0/16)はSINETを通じてインターネットへ経路が広告されているため，インターネット側から本学のアドレスへ向かうパケットはSINETへルーティングされる。したがって本学とSINETの接続に

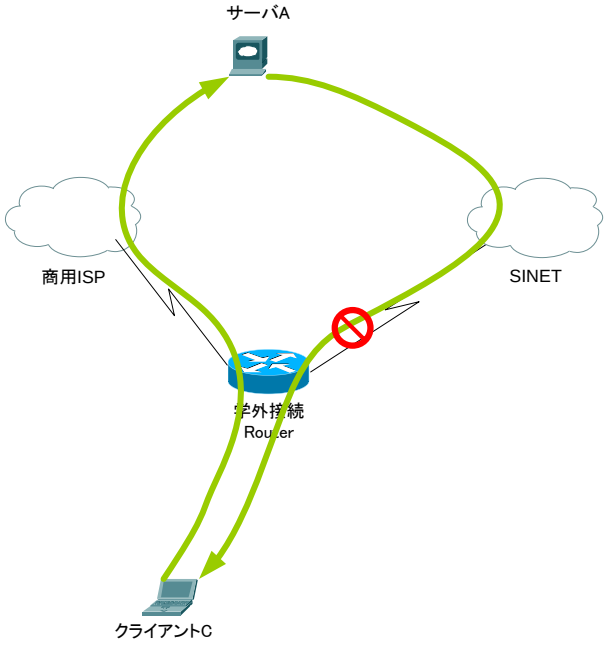

図 4　商用ISP経由でのアクセス(1)

問題が発生している場合はインターネット側から本学にはIPパケットは届かない(図 4)。つまり，SIENTダウン時に学内のクライアントCから商用ISP経由でインターネット上のサーバAにパケットを届けることは可能だが，サーバAからCへのパケットはSINETに向けてルーティングされてしまうために届かない。AからCへのパケットが届かないためにTCPのような双方向通信は成立しない。この問題を根本的に解決するためには，本学ネットワークへの経路を商用ISPからもインターネットへ広告する必要がある。しかし複数経路の広告を行うにはAS番号を取得し，BGPを使ってルーティング情報の交換を行う必要がある。しかし，経路の広告はインターネットに対して広範囲に影響を与えるため，運用には高度な知識と安定性が求められる。したがって本学でBGPの運用を行うのは現実的ではない。

より簡易に冗長化された上位ネットワークを利用する方法としてNAPT(Network Address Port Translation, IP Masquerade)を利用した方法がある。学内ネットワークから商用ISPにルーティングされたパケットに対してNAPTを適用し，パケットのソースアドレスを商用ISPから割り当てられたIPアドレスBに変更する(図 5)。

この方法では学内のクライアントCからのアクセスはNAPTを経由する際にソースアドレスがアドレスBに変更される。サーバAから見ればパケットの送信者は商用ISPのアドレスBに見えるため，Bへの応答パケットはSINET経由ではなく，商用ISPへルーティン

グされる。A から B へのルートが SINET を経由していなければ，SINET 停止時でも学内からインターネット接続の確保が可能となる。

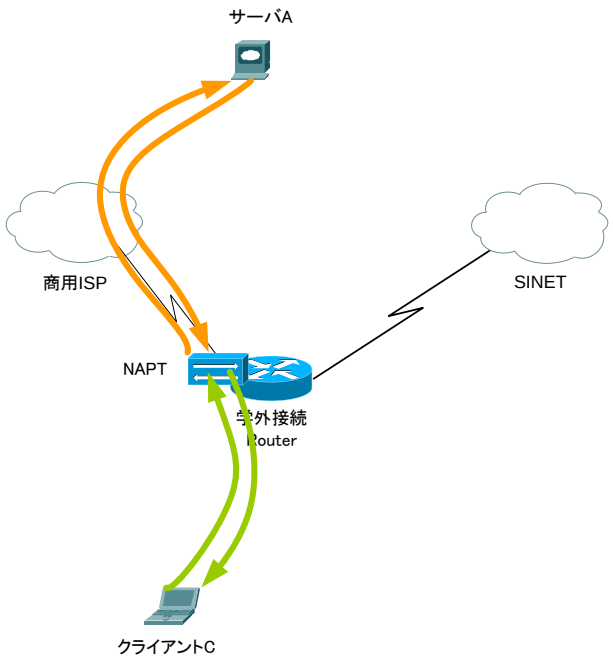

図 5　商用 ISP 経由でのアクセス(2)

3．2 HTTP トラフィックルーティング

次にどのようなパケットを商用 ISP へルーティングするのか考える。経路情報を上位 ISP と交換し，IP レベルでのマルチホーム接続を行っている場合，IP アドレスの宛先情報によりルータが自動的に最適な経路を選択できる。しかし NAPT を用いる場合，経路情報を持たないため，IP レベルでの最適な経路の選択ができず，別な情報を利用して経路を選ぶ必要がある。今回はネットワーク利用の大半を占める HTTP トラフィックに注目し，URL で示される相手のドメインにより経路選択することとした。SINET は学術研究用のネットワークであり，国内の多くの大学が参加しているため“ac. jp”ドメインにマッチすれば SINET，それ以外は商用 ISP へとルーティングする。ただし，いくつかのサイト(附属図書館が契約している電子ジャーナルなど)ではアクセスを学内ネットワークに制限しているため，そのようなサイトへのアクセスは SINET 経由になるよう除外ルールも適用できる必要がある。

4．実装

前節で述べた HTTP トラフィックのルーティングのフローチャートを図 6 に示す。本節ではこれらの処理の実装について述べる。

HTTP トラフィックのルーティングは

- HTTP Proxy(Squid-3.0)
- ポリシールーティング(RTX 1100)

を利用し，実現した。

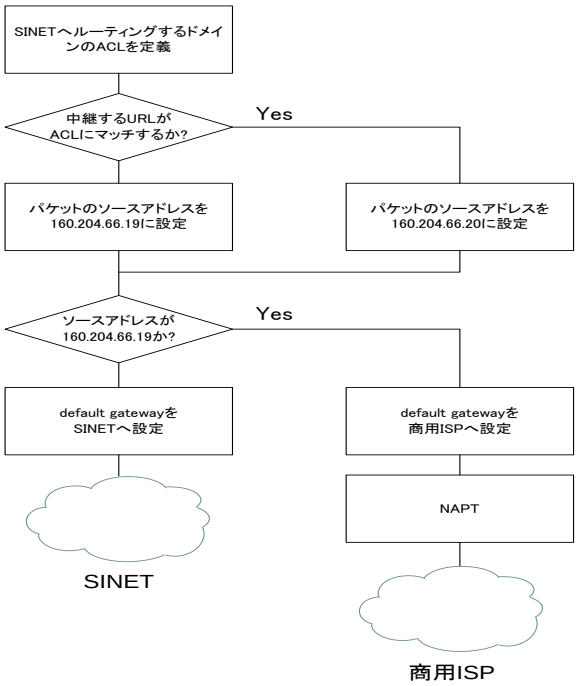

図 6　HTTP トラフィックのルーティング

4．1 HTTP Proxy

HTTP Proxy サーバは Squid を用いた。HTTP トラフィックのルーティングに用いたホスト(RedHat ES3)では，既に通常の HTTP Proxy サーバとして利用しており，パッケージで提供される Squid が 8080 ポートで稼働している。1 台のホストで複数の Squid を起動するにあたり，設定ファイルの衝突を避けるため，ソースから最新の Squid-3.0 をビルドし，/usr/local/squid/配下にインストールしたものを HTTP ルーティング用の HTTP Proxy として利用した。

Squid にはクライアントから送られてくる要求へのアクセス制御のため，Access Control List(ACL)と呼ばれる機能が提供されている [2]。ACL にはさまざまな条件を設定可能であるが，今回は HTTP の宛先により上位 ISP の切り替えを行うため，特定の宛先ドメインに対するリクエストにマッチする“dstdomain”を利用する。次にこの ACL にマッチする特定のドメイン宛の HTTP リクエストを学外ルータにて商用 ISP へルーティングするために必要な情報を付加する。今回はマッチしたリクエストに対して，“tcp_outgoing_address”を指定し，ACL にマッチしたリクエストを中継する際，ソースアドレスを変更する。こうすれば通常の HTTP リクエスト中継時と ACL にマッチしたリクエストではパケットのソースアドレスが異なる。学外接続ルータ

では，ソースアドレスの違いを利用し，後述するポリシールーティングによりパケットの送出経路を変更する。

図 7 に HTTP トラフィックルーティングに関連する squid の定義ファイルを示す。最初に SINET へルーティングすべき宛先にマッチする ACL を定義している。次に定義した ACL にマッチした場合，中継パケットのソースアドレスを 160.204.66.20 に設定する。ACL にマッチしない場合，中継パケットのソースアドレスは 160.204.66.19 になる。

この定義では，“ac.jp”にマッチする場合，無条件に SINET へルーティングされてしまう。そのため SINET ダウン時にはルールを変更する必要がある。

```
# These sites allow only access from 160.204.
acl mainichi dstdomain .g-search.or.jp
acl EBSCOhost dstdomain .ebscohost.com
acl LLBA dstdomain .csa.com
acl MathSciNet dstdomain .ams.org
acl JapanKnowledge dstdomain .jkn21.com
acl SpringerLink dstdomain .springerlink.com
acl WileyInterScience dstdomain .wiley.com
acl ScienceDirect dstdomain .sciencedirect.com
# Requests that matched ACL are routed to the SINET
tcp_outgoing_address 160.204.66.20 acjp
tcp_outgoing_address 160.204.66.20 mainichi
tcp_outgoing_address 160.204.66.20 EBSCOhost
tcp_outgoing_address 160.204.66.20 LLBA
tcp_outgoing_address 160.204.66.20 MathSciNet
tcp_outgoing_address 160.204.66.20 JapanKnowledge
tcp_outgoing_address 160.204.66.20 SpringerLink
tcp_outgoing_address 160.204.66.20 WileyInterScience
tcp_outgoing_address 160.204.66.20 ScienceDirect
# Other requests are routed to the ISP.
tcp_outgoing_address 160.204.66.19
```

図 7　Squid の定義

4．2 ポリシールーティング

一般的な IP パケットのルーティングは宛先アドレスに対する経路をルーティングテーブルから検索することで行われる。つまり同じ宛先であれば，同じ経路が割り当てられる。ポリシールーティングでは，経路の選択に宛先アドレスに加えてあらかじめ管理者の設定したポリシーに基づき対象パケットの経路を決定することができる。

学外接続ルータ（図 8）として利用している YAMAHA RTX1100 ではポリシーフィルターと経路情報の組み合わせでポリシールーティングを実現する [3]。

設定しているポリシーは

- パケットのソースアドレスが 160.204.66.19 なら商用 ISP を default gateway とする。それ以外のパケットは default gateway を SIENT とする。
- 商用 ISP がダウンしている場合は SINET を default gateway とする。

である。学外接続ルータで行っているポリシールーティング関連部分の定義を図 9 に示す。

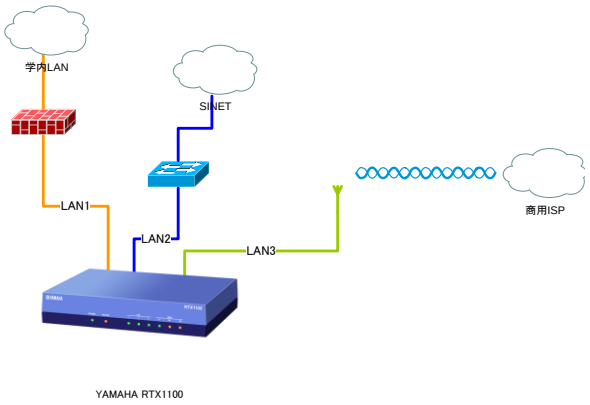

図 8　学外接続ルータ

```
ip route default gateway pp 1 filter 501 hide gateway 150.99.192.229
ip route 160.204.0.0/16 gateway 160.204.119.117
…
ip filter 501 pass 160.204.66.19 * * *
….
```

図 9　学外接続ルータの定義

4．3 Proxy の設定

HTTP トラフィックルーティングには HTTP Proxy サーバを利用している。そのため，商用 ISP を利用するためには利用者に適切な HTTP Proxy

http://proxy.naruto-u.ac.jp:3128/

を設定してもらう必要がある。ただし，このような指定をユーザに行ってもらうのは負担が大きい。また運用上 Proxy サーバの IP アドレスやポート番号を変更することもあり得ることも考え，今回は自動設定用の設定ファイルでのみ商用 ISP 用の Proxy サーバ情報を公開した。学内 LAN の利用者はブラウザの設定で「設定を自動設定する」が有効になっていれば自動的に適切な Proxy が設定される。

図 10 に本学で利用している Proxy 自動設定スクリプトを示す。スクリプトの内容は学内のサーバであれば Proxy を介せずに直接接続し，それ以外は Proxy としてトラフィックルーティング用 Squid（3128）を利用する。3128 が利用出来ない場合は従来の Squid（8080）を利用し，それも利用出来ない場合は直接接続する。

```
function FindProxyForURL(url, host)
{
    if (isPlainHostName(host) ||
        shExpMatch(host, "*.naruto-u.ac.jp") ||
        isInNet(host, "160.204.0.0", "255.255.0.0") ||
        isInNet(host, "127.0.0.0", "255.0.0.0") ||
        shExpMatch(host, "localhost¥.?*"))
        return "DIRECT";
    else
        return "PROXY 160.204.66.20:3128; PROXY 160.204.66.20:8080; DIRECT";
}
```

図 10　Proxy 自動設定スクリプト

5. 考察

2007年11月1日0時0分から2007年12月31日23時59分までの期間における学外接続ルータのトラフィックを図に示す。これらのグラフはcactiというフリーのツールによりSNMPによって取得された値をグラフ化したものである。

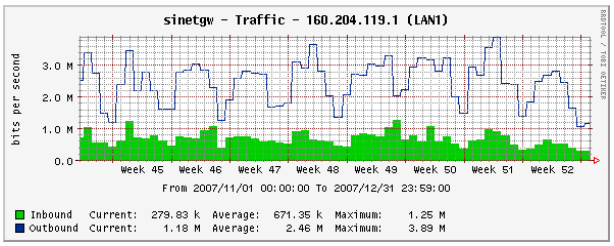

図 11 学外接続ルータトラフィック(LAN1)

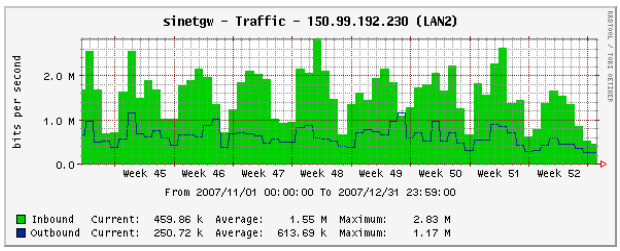

図 12 学外接続ルータトラフィック(LAN2)

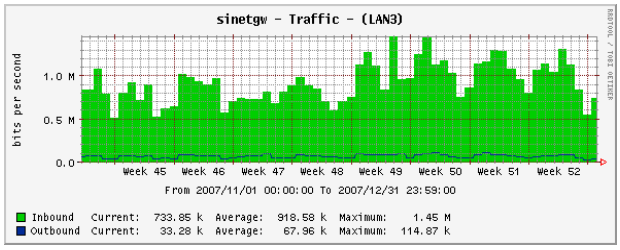

図 13 学外接続ルータトラフィック(LAN3)

図 11 の示す LAN1 は学内 LAN と学外接続ルータを接続するインタフェースである。つまり学内とインターネットとのトラフィックを示している。図 12 の示す LAN2 は SINET に接続されたインタフェースであり，学内と SINET とのトラフィックを示している。図 13 の示す LAN3 は商用 ISP に接続されたインタフェースであり，学内と商用 ISP とのトラフィックを示している。またこれらの図で示される Inbound，Outbound の値はルータへの Inbound，Outbound の意味であり，学内への Inbound，Outbound を意味しないことに注意して欲しい。学内への Inbound，Outbound で考えた場合，LAN1 の Inbound，Outbound の値が逆転する。

表 1 各インタフェースのトラフィック(平均)

	Inbound	Outbound
LAN1	0.67	2.46
LAN2(SINET)	1.55	0.61
LAN3(ISP)	0.92	0.07

図 11，図 12，図 13 のグラフから各インタフェースのトラフィックの平均値を求めたものを表 1 に示す。インターネットからの Inbound トラフィックに注目すると，商用 ISP は平均 0.92Mbps となっている。これは学内への Inbound トラフィック 2.46Mbps の約 37%になる。商用 ISP には Proxy サーバを経由する HTTP リクエストの一部をルーティングしているだけであるが，そのレスポンスによってこれだけのトラフィックがもたらされている。

このように HTTP トラフィックのうち，一部のリクエストを商用 ISP へルーティングするだけでも約 37%のトラフィックが商用 ISP へ分散されたことは今回の試みが負荷分散に有効であり，マルチホーム接続で拡大されたインターネットへの帯域をうまく活用できていることを示していると考える。

表 2 に proxy サーバ上で稼働している 2 つの Squid における平均サービス時間(秒)を示す。2 つの Squid は稼働時間やバージョンが異なる(Squid for ISP は 3.0，Squid for SINET は 2.5)ため，単純に比較出来ないが，商用 ISP 経由でコンテンツを取得する Squid for ISP の方がレスポンスがよい。Squid for ISP はバージョンがより新しく実装がチューニングされている可能性も否定できないが，商用 ISP 経由の方が早くコンテンツを取得できているようである。SINET は徳島ノードを経由して松山地域のルータで SINET バックボーンに接続されている。学外ルータから松山ルータまでの経路で常に 20ms 程度の遅延があり，サービス時間に影響していると考える。

表 2 Squid の平均サービス時間

	Squid for ISP	Squid for SINET
HTTP Requests (All)(5min)	0.02899	0.15048
HTTP Requests (All)(60min)	0.01847	0.09219
Cache Misses(5min)	0.07825	0.22004
Cache Misses(60min)	0.11465	0.19742

6. まとめ

マルチホーム接続により，本学とインターネットの接続は冗長化され，帯域も拡大された。マルチホーム接続を運用の負担を増やすことなく有効活用するため，HTTP トラフィックを Proxy サーバによりルーティングする手法を試

行した。その結果，HTTP トラフィックの一部のみでも商用 ISP に負荷を分散させることにより，SINET 側の負荷が従来よりも下がり，より快適なインターネット接続を利用者に対して提供できることが分かった。

現在の構成では，“ac.jp”ドメインへのアクセスはすべて SINET 側へルーティングしているため，SINET ダウン時にはアクセスできなくなる。“ac.jp”ドメインも含めて SINET ダウン時でもアクセスできるように Proxy サーバの構成や設定を見直す必要がある。また今回の手法では Proxy の自動設定を有効にしている利用者のみが商用 ISP へのルーティングが行われる。しかし，学内には Proxy を経由せずに従来通り SINET を経由している HTTP トラフィックもまだ多い。今後，より多くの利用者に Proxy サーバを利用してもらうために透過 Proxy の組み合わせや Proxy を設定する利点の広報が必要である。また，HTTP トラフィック以外にも商用 ISP を利用することで負荷分散が図れる物があれば利用を進めていきたい。

今回は学内からインターネットへの Outbound のみを対象としたが，インターネットから学内への Inbound においても商用 ISP をうまく活用する方法を考える必要がある。特に学内のメールサーバや Web サーバへの Inbound トラフィックが商用 ISP 経由でも可能になれば，安定したサービスの提供という観点からは非常に有効である。商用 ISP には 1 つの固定グローバルアドレスを取得しており，今後は DNS との組み合わせなどで Inbound トラフィックの分散も図りたいと考えている。

参考文献

1. **NTT 西日本.** B フレッツ ワイヤレスタイプ. (オンライン)
http://flets-w.com/bflets/service_menu/wireless/index.html.

2. **The Squid project.** ACL. squid-cache. (オンライン)
http://www.squid-cache.org/Versions/v3/3.0/cfgman/acl.html.

3. **ヤマハ.** コマンドリファレンス. (オンライン) 2007 年.
http://www.rtpro.yamaha.co.jp/RT/manual/Rev.10.00.16/Cmdref.pdf.